Time Impulsion Based Data Security in Clouds

Mahejabin Patel
Computer Department, Savitribai Phule Pune University
SVPMCOE,Malegaon(Bk),Baramati,dist-Pune,Maharashtra,India
patelmahejabin2514@gmail.com

Shraddha Londhe
Computer Department, Savitribai Phule Pune University
SVPMCOE,Malegaon(Bk),Baramati,dist-Pune,Maharashtra,India
shraddhalondhe76@gmail.com

Nital Shinde
Computer Department, Savitribai Phule Pune University
SVPMCOE,Malegaon(Bk),Baramati,dist-Pune,Maharashtra,India
NitalShinde2595@gmail.com

Shweta Mulik
Computer Department, Savitribai Phule Pune University
SVPMCOE,Malegaon(Bk),Baramati,dist-Pune,Maharashtra,India
mulikshwetaaa@gmail.com

Prof V.V.Sawant
Computer Department, Savitribai Phule Pune University
SVPMCOE,Malegaon(Bk),Baramati,dist-Pune,Maharashtra,India
VanitaVSawant@gmail.com

Abstract: Cloud Computing is evolving in sector of Information Technology,although it has tremendous approach in terms of providing storage facility,cost efficiency,using third party tools, yet Security of data in clouds is point of concern,as data owner is different than administrator of cloud and hence data outsourced by data owner may be migrated or misued in clouds.In this paper, Key Policy Time Specified Attribute Based Encryption scheme(KPTSABE) is proposed to solve issue regarding data Security in clouds with time impulsion on access of data.

Keywords—Security,Cloud Computing,Secure Self Destructing,Fine grained Access Control,Sensitive Data

I. Introduction

With the enormous development of negotiable cloud offerings,it is yet raising to vulnerable use of it. Because it is not sustainable to provide complete life-cycle security, in particular when we share sensitive information on cloud servers.

The shared data in cloud servers, however, usually comprise user's vital information and needs to be well defended. As the ownership of the data is aparted from the administration of them, the cloud servers may move users data to other cloud servers in outsourcing them in cloud searching. Therefore, it becomes a big dispute to protect the secrecy of those shared data in cloud, especially in cross cloud and big data environment. In order to meet this challenge, it is essential to design a encompassing solution to support user-defined authorization period and to accomodate fine grained access control during this period. The shared data should be self-destructed after the data owner defined expiration time.

II. *Literature Survey*

Following are the Existing System:

A. *Attribute Based Encryption(ABE)[6]:*
Technique used is Key-Policy Attribute Based Encryption(KP-ABE). Based on traditional public key encryption it achieves flexible one to many encryption. Due to lack of time constraint it does not provide user defined authorization period.

B. *CP-ABE[5] :*
Linear Secrete Sharing Scheme (LSSS). It provide access structure while the private key contains a set of attributes. Security proof was only construct under the generic group model.

C. *Vanish[10]:*
Vanishing data object (VDO) ,Distributed Hash Table(DHT) & It enables users to control over the lifecycle of the sensitive data. Ciphertext is not destucted ,it does not supporting for fine-grained access control

D. *Secure self destructing Scheme For electronic data (SSDD)[2]:*
Technique used is Distributed Hash table(DHT),
Ciphertext is destucted and also key is destucted. Does not provide user defined time intervals .

E. *IBE-based Secure Self-destruction (ISS)[6]:*

Attribute Based Encryption Algorithm is used for cryptography. Ciphertext is destucted And also it supports for fine-grained access control. It does not provide full lifecycle privacy protection and does not support user-defined time intervals.

F. Full lifecycle for Privacy Protection(FullPP) [6]:

Combine different cryptographic techniques with the DHT network .Ciphertext is destucted by providing full lifecycle privacy protection. It does not support accurate user-defined time intervals.

III.CONTRIBUTION

We present a KP-TSABE scheme, that is a novel approach to understand self-destructing scheme for data sharing in cloud computing. We first introduce the need of KP-TSABE, describe the model of KP-TSABE and give the security version of it. Then,we prove that the KP-TSABE scheme is secure. Specially, KP-TSABE has the following advantages with respect to protection and fine-grained access control in comparison to other comfortable self-destructing schemes.

1) KP-TSABE accompain the characteristic of user defined authorization and ensures that the essential information cannot be read earlier than its release time and after its expiration time.

2) KP-TSABE does not require the convenient assumption of “No attacks on VDO earlier than it expires”.

3) KP-TSABE is able to provide fine-grained access control during the authorization duration and to destruct data/information data owner specified expiration time without any human interference.

4) KP-TSABE is approved to be secure below the usual version by way of the usage of the l-bilinear DiffieHellman assumption and elgamal algorithm.

IV. SYSTEM ARCHITECTURE

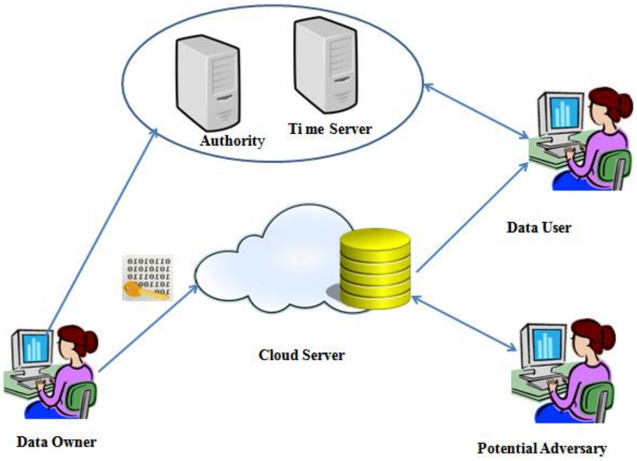

Fig. 1. System Architecture

- **Data Owner:** Data owner can supply data or files that contain some vital information, which are used for sharing with his/her friends(datausers). All these shared data are send to the cloud servers to data store.
- **Authority:** It is an necessary entity which is liable for creating, assigning and managing all the private keys, and is trusted by all the other entities concer -ned with the system.
- **Time Server:**It is a time recommendation server without any interaction with other entities involved in the system. It is responsible for a exact deliver time specification.
- **Data Users:**Data users are some people who passed the identity validation and access to the data outsourced by the data owner. The shared data can only be accessed by the authorized users during its authorization period.
- **Cloud Servers:**It contains almost limitless storage space which is capable to store and manage all the data or files in the system. Other entities with limited storage space can store their data to the cloud servers.

V. MODEL OF KP-TSABE

The Key Policy-Time Specified Attribute Based Encryption (KP-TSABE) scheme can be depicted as postulation of following functions using Bilinear Diffie Hellman algorithm for key exchange[6] and Elgamal algorithm, for encryption:

1. **Setup(ƛ,U)** : It takes input as security parameters and attribute set , authority provide Master Secret Key (MSK) and generate parameters as Output.
   i.e
   O={param,MSK}
   where,
   param={g1, g2,g3}
   where ,
   g1,g2, g3 are randomly selected parameters
   MSK=, **a**
   where , **a** generated using param
2. **KeyGen(OKpri ,UKpri):** This function takes MSK access tree as input and Generate owner’s and users private ,public and encryption Key.
   i.e
   OKpri is Owner private key
   UKpri is Users private key
   OKpub is Owner public key
   UKpub is Users public key
   Ek is encryption key
   OKpri and UKpri are randomly selected.
   h is primitive root or genrator.
   g is prime number.
   h=g^msk
   OKpub = (g^OKpri) mod h
   UKpub = (g^UKpri) mod h
   Ek = UKpub ^ (OKpri) mod h
   O={OKpub,UKpub,Ek }
3. **Encrypt(Ek,M) : The** input to this function is encryption key **(Ek)** and Message **(M)** using this input the owners data/files is encrypted and then outsourced to cloud server.

where,
M is message to be encrypted.
CT is ciphertext
CT= Ek :(M) mod h
O={CT}

4. **Decrypt(CT,UKpri):**Input to this function is cipher text i.e encrypted message and User private key,to Generate decryption key i.e equal to encryption key & Using decryption key data/file get decrypted.
i.e

Dk = OKpub^(UKpri) mod h
Dk should be equal to Ek
Dk .x mod h=1
x is number such that after computation answer is 1.
M=x.CT mod h
O={M}

5. **Time(id,Ts):** where id is file id and Ts is time specified by data owner, if tb < tc < te then T`= ts
where,
tb :start time specified by Owner
tc :current time of User
te :end time specified by Owner
T`: is time specified to User.

VI. SECURITY MODEL FOR KP-TSABE

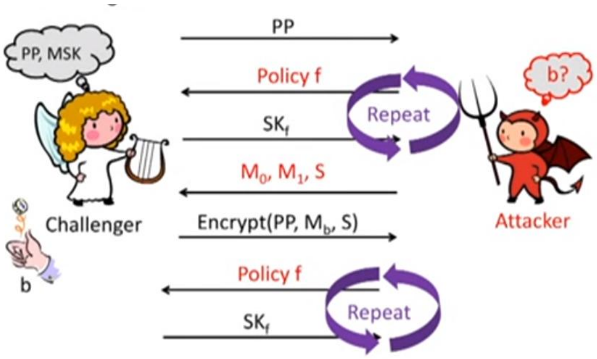

Fig. 1. Security Model for KP-TSABE

Here,challenger is authority responsible to provide attacker resistant system and attacker is potential adversary trying to attack the system with its malicious act.

Attacker always try to guess what would be secret keys to get access to vital data outsourced by data owner. KP-TSABE is secure in these terms as authority generates private key of data owner and user randomly,system is NP Complete due to randomization used to generate the keys.

Hence the probability of attack is less or attacker is not capable to attack on system i.e KP-TSABE is Secure Scheme.

VII. CONCLUSIONS

It helps us to understand ,Key-Policy Time Specified Attribute Based Encryption(KP-TSABE) approach for secure data self destruction stored in cloud servers is efficient scheme to provide fine grained access control to data Owner.

ACKNOWLEDGMENT

It gives us great pleasure in presenting KPTSABE scheme for “Time Impulsion Based Data Security in Clouds” we would like to take this opportunity to thank our internal guide Prof. Sawant.V.V and all teachers for giving us all the help and guidance we needed.we are really grateful to them for their kind support.we appreciate all valuable suggestions given and queries raised by her which really helped us in exploring project in deep.

We are also grateful to Prof.Mhaske.V.D, Head of Computer Engineering Department,SVPM COE for her indispensable support, suggestions.

REFERENCES

1. A. Shamir, How to share a secret, Communications of the ACM, vol. 22, no. 11, pp. 612613, 1979.
2. A. Sahai and B. Waters, Fuzzy identity-based encryption, in Advances in CryptologyEUROCRYPT 2005, ser. LNCS, vol.7371. Springer, 2005, pp. 457473.
3. A. F. Chan and I. F. Blake, Scalable, server-passive, useranonymous timed release cryptography, in Proceedings of the International Conference on Distributed Computing Systems. IEEE, 2005, pp. 504513.
4. A. W. Dent and Q. Tang, Revisiting the security model for timed-release encryption with pre-open capability, in Proceedings of the Information Security. Springer, 2007, pp. 158174.
5. B. Waters, Ciphertext-policy attribute-based encryption: An expressive, e_cient, and provably secure realization, PublicKey CryptographyPKC 2011, pp. 5370, 2011
6. J. Xiong, Z. Yao, J. Ma, F. Li, and X. Liu, A secure selfdestruction scheme with ibe for the internet content privacy, Chinese Journal of Computers, vol. 37, no. 1, pp. 139150, 2014.
7. J. Reardon, D. Basin, and S. Capkun, Sok: Secure data deletion, in Proceedings of the 34th IEEE Symposium on Security and Privacy. IEEE, 2013, pp. 115.
8. J. Reardon, H. Ritzdorf, D. Basin, and S. Capkun, Secure data deletion from persistent media, in Proceedings of the 2013 ACM Conference on Computer and Communications Security
9. K. G. Paterson and E. A. Quaglia, Time-speci_c encryption,in Security and Cryptography for Networks. Springer, 2010, pp. 116.
10. R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, Vanish Increasing data privacy with self-destructing data, in Proceeding of the 18th USENIX Security Symposium, 2009, pp. 299315.
11. S. Yu, C. Wang, K. Ren, and W. Lou, Achieving secure, scalable, and _ne-grained data access control in cloud computing, in Proceedings of the 29th IEEE International Conference on Computer Communications. IEEE, 2010, pp. 19.